REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-25 are pending in the application. The Examiner additionally stated that claims 1-25 are rejected. By this communication, claims 1-25 stand for further examination without amendment. Hence, claims 1-25 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-25 under 35 U.S.C. 103(a) as being unpatentable over Kessler, US6789147 (hereinafter, "Kessler"), in view of Colavin, U.S. Publication No. 20040103263 (hereinafter, "Colavin"), and further in view of Miller, US6081884 (hereinafter, "Miller"). Applicant respectfully traverses the Examiner's rejections.

Claim 1 recites:

1. An apparatus for performing cryptographic operations, comprising:

an x86-compabitle microprocessor, comprising:

fetch logic, configured to receive a single, atomic cryptographic instruction, wherein said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation, and wherein said single, atomic cryptographic instruction prescribes one of a plurality of cryptographic algorithms;

algorithm logic, operatively coupled to said single, atomic cryptographic instruction, configured to direct said x86-compatible microprocessor to execute said encryption operation according to said one of a plurality of cryptographic algorithms; and

execution logic, operatively coupled to said algorithm logic, configured to execute said one of the cryptographic operations, wherein said execution logic comprises a cryptography unit for executing a plurality of cryptographic rounds required to complete said encryption operation.

In reply to the Examiner's argument's submitted in the instant Office Action, the Examiner argues that "Colavin discloses that the co-processor is more than just a simple co-processor that 'only possesses those capabilities needed to perform security operations,' but instead is reconfigurable to provide program executions with very high instruction level parallelism ([0084]). This argument is not persuasive because Colavin's coprocessor, like a VLIW processor, has a large number of processing elements and can execute programs with very high instruction level parallelism and, as one skilled in the art will appreciate, programs with very high instruction level parallelism exhibit the trait that many of the operations in the executed programs can be performed *simultaneously*, that is, those instructions which are not data dependent, and can thus be executed simultaneously. Furthermore, as one skilled in the art will affirm, fields such as graphics and scientific computing exhibit high degrees of instruction level parallelism. However, workloads such as *cryptography exhibit much less parallelism*. Applicant respectfully notes that the present invention features a *single, atomic cryptographic instruction*, and not a plurality of non-data dependent instructions. Thus, it is respectfully submitted that the Colavin reference is neither relevant nor material as a reference. To combine the teachings of Kessler and Colavin would lead one skilled in the art to posit a multiple coprocessors (multiple execution units) of the form of Kessler which could simultaneously perform independent and non-data-dependent security operations, but would not yield that which is recited.

The Examiner argues that the co-processor of Kessler as modified by Colavin would not be a mere security co-processor (as argued by the Examiner in combining Kessler and Colavin), and thus it could have been obvious for the co-processor described in Kessler to implement the x86 instruction set because of its wide acceptance as taught by Miller. This argument is not persuaded because, as is noted above, the combination of Kessler

and Colavin does not teach the recited limitations. It is conceded that Colavin's processor may implement the x86 instruction set because of its wide acceptance, however, as noted above, Kessler and Colavin do not teach a processor capable of executing a single, atomic cryptographic instruction as is claimed.

The Examiner argues that it would have been "obvious. . . for the co-processor of Kessler to execute the actual application program as described by Colavin in order to efficiently execute programs with high instruction level parallelism as taught by Colavin." This argument is not persuasive because the invention according to the instant claims do not exhibit high instruction level parallelism, as one skilled in the art will concur, for a *single, atomic cryptographic instruction* is claimed, and it is well-know that cryptographic operations do not exhibit high instruction level parallelism and are highly data-dependent.

Nowhere do the cited references disclose **a single, atomic cryptographic instruction, wherein said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation**, as is recited in claim 1.

The Examiner argued that because Miller teaches that the x86 instruction set has been widely accepted because of its compatibility with a large amount of software, it would have been obvious to one of ordinary skill in the art at the time of invention for the co-processor described in Kessler to implement the x86 instruction set. Applicant respectfully disagrees with these points because *nowhere* do these references suggest that use of an x86-compatible microprocessor for purposes of performing an encryption operation. Applicant submits that Kessler teaches a security co-processor interface, for performing security operations. Such an interface does not constitute the functions that are commensurate with implementation of the x86 instruction set, which would yield an x86-compatible microprocessor, as is disclosed in the instant specification. Applicant respectfully asserts that an x86-compatible microprocessor is a well-known term of art and is sufficiently supported within the instant disclosure to include, as Miller discloses "compatibility with a large amount of software," among other features. Thus, it does not

follow that one skilled would be even remotely motivated to implement the x86 instruction set on the co-processor of Kessler for Kessler's co-processor only possesses those capabilities needed to perform security operations. And as noted above, the combination of Kessler and Colavin would not teach the noted limitation, but would rather teach parallel versions of Kessler's security co-processor for performing independent security operations.

In addition, Applicant submits that it is difficult to find any practical combination of Kesseler, Colavin, and Miller, which would result in the limitation cited above. The only contribution that Miller makes to the argument is that the x86 instruction set is well-known and widely accepted. Yet, none of the references, alone or in combination, teach, hint, suggest, or allude to a single, atomic cryptographic instruction that is of the x86 instruction format.

Furthermore, Applicant submits, again, that the point that Colavin makes in the Abstract and paragraph [0018] is that *identical processing elements* in a coprocessor configured in parallel can be used to accelerate execution of portions of a program having high instruction level parallelism, which not germane to cryptographic operations due to the high data dependency requirements in sub-operations.

Applicant has thoroughly studied the teachings of Kessler, Colavin, and Miller, both alone and in combination, and finds that Kessler and Colavin fail to teach any form of **an x86-compatible microprocessor**, as is recited in claim 1. As has been previously submitted, Kessler teaches a security co-processor interface. Colavin teaches clustered VLIW processing elements, coupled by a runtime reconfigurable inter-cluster interconnect to form a coprocessor executing only those portions of a program having high instruction level parallelism. (Abstract). And Miller only adds that the x86 instruction set has been widely accepted because of it's compatibility with a large amount of software. The combination of these three references do not yield anything practical for one skilled in the microprocessor arts. Furthermore, the combination of these references fail to suggest **an x86-compatible microprocessor** that comprises, *inter alia*, **a single, atomic cryptographic instruction, wherein said single, atomic cryptographic**

instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation, as is recited in claim 1.

Thus, for at least the above reasons, it is respectfully asserted that claim 1 is patentably distinct and non-obvious over the cited art. Consequently, it is requested that the rejection be withdrawn.

Claim 21 recites substantially the same limitations as have been argued above as being allowable over the combination of Kessler, Colavin, and Miller. Accordingly, it is requested that the rejection of claim 21 be withdrawn as well.

With respect to claims 2-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-15.

With respect to claims 22-25, these claims depend from claim 21 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 22-25.

As per claim 16, substantially the same limitations are recited as have been argued above with regard to claims 1 and 21, the exception being that claim 16 recites that the single atomic cryptographic instruction prescribes a decryption operation. Consequently, it is requested that the rejection be withdrawn since the recited limitations are not taught, contemplated, or suggested by the combination of Kessler, Colavin, and Miller.

With respect to claims 17-20, these claims depend from claim 16 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 16-20.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-25 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

04/05/2010

Date: _____